



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,461	01/31/2002	Timothy David Dodd	05456.105036	2190

20786 7590 11/02/2005

KING & SPALDING LLP
191 PEACHTREE STREET, N.E.
45TH FLOOR
ATLANTA, GA 30303-1763

EXAMINER

TOLENTINO, RODERICK

ART UNIT PAPER NUMBER

2134

DATE MAILED: 11/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/066,461	Applicant(s) DODD ET AL.	
	Examiner Roderick Tolentino	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01/31/2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 - 49 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1 - 49 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 September 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims 1 – 49 are pending.

Claim Rejections - 35 USC § 101

[001] 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

[002] Claims 1 – 49 are rejected under 35 U.S.C. 101 because the claimed invention lacks patentable utility. According to MPEP 2106 the fact that the claim may satisfy the utility requirement of 35 U.S.C. 101 does not mean that a useful result is achieved under the practical application requirement. For example, a claim directed to a word processing file stored on a disk may satisfy the utility requirement of 35 U.S.C. 101 since the information stored may have some "real world" value. However, the mere fact that the claim may satisfy the utility requirement of 35 U.S.C. 101 does not mean that a useful result is achieved under the practical application requirement. The claimed invention as a whole must produce a "useful, concrete and tangible" result to have a practical application. The present invention does not create a useful, concrete or tangible result. The invention creates a risk value that is not used for any practical use and thus is considered to lack utility.

Claim Rejections - 35 USC § 112

[003] The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

[004] Claims 6 and 7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

[005] As per claim 6, it is indefinite as to what the asset value is obtaining from an operating system, or system service or the system vulnerabilities. It is as best understood the examiner, to assume the value being obtained is the vulnerability value of the system or service is being analyzed.

[008] As per claim 7, the term "potential" in claim 7 is a relative term which renders the claim indefinite. The term "potential" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The term "potential" in reference to the access available to a system is not set or defined value and leaves the claim open to interpretation.

Claim Rejections - 35 USC § 102

[009] The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

Art Unit: 2134

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

[010] The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

[011] Claims 1, 5 - 7, 9, 10, 18 – 20, 23 – 31, 34 – 37 and 43 - 49 are rejected under 35 U.S.C. 102(e) as being anticipated by Fox et al. U.S. Patent No. (6,883,101).

[012] As per claim 1 Fox discloses selecting a vulnerability for the system (Fox, Col. 3 Lines 18 – 21), obtaining an asset value for the system (Fox, Col. 3, Lines 31 – 36), determining an exploit probability for the vulnerability (Fox, Col. 9, Lines 43- 45), obtaining a severity value for the vulnerability (Fox, Col. 9, Lines 17 – 20), computing a risk value for the vulnerability based on at least one of the asset value, the exploit probability, and the severity value (Fox, Col. 10 Lines 5 – 10, 15 – 21), if there are additional vulnerabilities associated with the system, repeating the foregoing steps to compute risk values for the additional vulnerabilities (Fox, Col. 10, Lines 23 – 27) and calculating a security score for the system based on at least one of the risk values associated with the system (Fox, Col. 10, Lines 30 – 36).

Art Unit: 2134

[013] As per claim 5 calculating a group security score for a group of systems based on individual security scores for each of the systems (Fox, Col. 9 Lines 66 – 67, Col. 10 Lines 1 – 22).

[014] As per claim 6 Fox discloses the asset value is obtained from at least one of an operating system, a system service and the system vulnerabilities (Fox, Col. 5 Lines 19 – 46, Col. 6 Lines 20 – 23).

[015] As per claim 7 Fox discloses a severity value based on the potential access available to the system from exploiting the vulnerability (Fox, Col. 9, Lines 13 – 21).

[016] As per claim 8 Fox discloses the step of calculating a risk value which multiplies the asset value, the probability of exploit and the severity value (Fox, Col. 10, lines 5-36).

[017] As per claim 9 Fox discloses a step of calculating a security score comprises placing a risk value on a banded scale (Fox, Col. 9, Lines 61 – 65, Col. 10, Lines 23 – 36).

[018] As per claim 10 Fox discloses a computer-readable medium having computer-executable instructions (Fox, Col. 3, Lines 52 – 57).

[019] As per claim 18 Fox discloses receiving an asset value from the security audit system for an element with which the vulnerability is associated (Fox, Col. 3, Lines 31 – 36), receiving an exploit probability value for the vulnerability from the security audit system (Fox, Col. 3, Lines 31 – 36, Table 1 and 2), receiving a severity value from the security audit system (Fox, Col. 3, Lines 31 – 36, Table 1 and 2, Fig. 8B), and computing

Art Unit: 2134

a risk value for the vulnerability, the computation comprising at least one of the asset value, the exploit probability value, and the severity value (Fox, Col. 10, Lines 5 –36).

[020] As per claim 19 Fox discloses computing a risk value for additional vulnerabilities associated with the element by repeating the foregoing steps (Fox, Col. 3 Lines 32 –36).

[021] As per claim 20 Fox discloses the step of calculating a security score from at least one of the risk values associated with the element (Fox, Col. 10, Lines 5 –36).

[022] As per claim 23 Fox discloses the step of calculating a group security score for a group of elements based on individual security scores (Fox, Col. 9 Lines 66 – 67, Col. 10 Lines 1 – 22).

[023] As per claim 24 Fox discloses an asset value is based on at least one of a host operating system, a host service, and the host vulnerabilities (Fox, Col. 5 Lines 19 – 46, Col. 6 Lines 20 – 23).

[024] As per claim 25 Fox discloses a severity value is based on the potential access available to the network from exploiting the vulnerability (Fox, Col. 9, Lines 13 – 21, Table 1, section 3).

[025] As per claim 26 Fox discloses a step of calculating a risk value comprises multiplying the asset value, the probability of exploit value, and the severity value (Fox, Col. 10, lines 5- 36).

[026] As per claim 27 Fox discloses the step of calculating a security score comprises placing a risk value on a banded scale (Fox, Col. 9, Lines 61 – 65, Col. 10, Lines 23 – 36).

Art Unit: 2134

[027] As per claim 28 Fox discloses a computer-readable medium having computer-executable instructions for performing the steps (Fox, Col. 3, Lines 52 – 57).

[028] As per claim 29 Fox receiving a vulnerability for the element, the vulnerability being identified by a security audit system (Fox, Col. 3, Lines 32 – 36), receiving an asset value for the element from the security audit system, wherein the asset value is based on at least one of an operating system, an element service, and the element vulnerabilities (Fox, Col. 10, Lines 5 – 36), receiving an exploit probability value for the vulnerability from the security audit system (Fox, Col. 6 Lines 20 – 24), receiving a severity value from the security audit system (Fox, Col. 5 Lines 19 – 46, Col. 6 Lines 20 – 23) and computing a risk value for the vulnerability, the computation comprising at least one of the asset value, the exploit probability value, and the severity value (Fox, Col. 10, Lines 5 – 36).

[029] As per claim 30 Fox discloses the step of computing a risk value for additional vulnerabilities associated with the element by repeating the foregoing steps (Fox, Col. 3 Lines 32 – 36).

[030] As per claim 31 Fox discloses a step of calculating a security score from at least one of the risk values associated with the element (Fox, Col. 10, Lines 5 – 36).

[031] As per claim 34 Fox discloses a step of calculating a group security score for a group of elements based on individual security scores (Fox, Col. 9 Lines 66 – 67, Col. 10 Lines 1 – 22).

Art Unit: 2134

[032] As per claim 35 Fox discloses a calculating a risk value comprises multiplying the asset value, the probability of exploit value, and the severity value (Fox, Col. 9 Lines 66 – 67, Col. 10 Lines 1 – 22).

[033] As per claim 36 Fox discloses a step of calculating a security score comprises placing a risk value on a banded scale (Fox, Col. 9, Lines 61 – 65, Col. 10, Lines 23 – 36).

[034] As per claim 37 Fox discloses a computer-readable medium having computer-executable instructions for performing the steps (Fox, Col. 3, Lines 52 – 57).

[035] As per claim 43 Fox discloses a manager software module operable for selecting a vulnerability for a host, (Fox, Col. 5 Lines 50 – 57), a storage module operable for storing an asset value for the host, an exploit probability for the vulnerability, and a severity value for the vulnerability (Fox, Col. 8, Lines 24 – 26, Fig. 3 Item 166), and a computation module operable for computing a risk value (Fox, Col. 3, Lines 52 – 57).

[036] As per claim 44 Fox discloses an asset value for the host is based on at least one of the host's operating system, the host's services, and the host's vulnerabilities (Fox, Col. 5 Lines 19 – 46, Col. 6 Lines 20 – 23).

[037] As per claim 45 Fox discloses computing the risk value is based on at least one of the asset value, the exploit probability, and the severity value (Fox, Col. 10 Lines 5 – 10, 15 – 21).

[038] As per claim 46 Fox discloses the computation module is further operable for computing risk values for multiple vulnerabilities (Fox, Col. 5, Lines 48 – 57).

Art Unit: 2134

[039] As per claim 47 Fox discloses computing a security score from multiple vulnerabilities (Fox, Col. 9 Lines 38 – 45).

[040] As per claim 48 Fox discloses computation module computes a security score by placing multiple risk values on a banded risk scale (Fox, Col. 9, Lines 61 – 65, Col. 10, Lines 23 – 36).

[041] As per claim 49 Fox discloses a computation module computing a group security score from multiple security scores (Fox, Col. 9 Lines 66 – 67, Col. 10 Lines 1 – 22).

Claim Rejections - 35 USC § 103

[042] The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

[043] Claims 2, 3, 11 – 17, 21, 22, 32, 33 and 38 - 42 are rejected under 35 U.S.C.

103(a) as being unpatentable over Fox et al. U.S. Patent No. (6,883,101) in view of

Nessus Scan Report

(<http://web.archive.org/web/20000301233806/http://www.nessus.org/demo/report.html>,

March 01, 2000).

[044] As per claim 2 Fox Fails to disclose calculating an adjusted risk value as a function of the risk and a fix difficulty value. However, Nessus teaches calculating an

adjusted risk value as a function of the risk and a fix difficulty value (Nessus, Page 3 section 3, solutions and risk factor).

[045] At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Nessus' method of determining risk and fixability with Fox's system for assessing security in a network, because it offers the advantage of displaying the vulnerability to a system (Nessus, Page 3 section 3).

[046] As per claim 3 Fox as modified discloses calculating an adjusted security score for the system based on at least one adjusted risk value (Fox, Col. 4 Lines 13 – 20).

[047] As per claim 11 Fox teaches selecting a vulnerability for the host, the vulnerability being identified during a security scan (Fox, Col. 3, Lines 18 – 21), obtaining an asset value for the host, the asset value obtained from at least one of a host operating system, a host service, and the host vulnerabilities (Fox, Col. 3 Lines 31-36), determining an exploit probability for the vulnerability, the exploit probability indicating the likelihood that the vulnerability will be exploited to compromise the host (Fox, Col. 9, Lines 43 – 45), obtaining a severity value for the vulnerability, the severity value characterizing the potential damage that can be done from exploiting the vulnerability (Fox, Col. 9, Lines 17- 20), computing a risk value for the vulnerability based on at least one of the asset value, the exploit probability, and the severity value (Fox, Col. 10 Lines 5 –10, 15 – 21), if there are additional vulnerabilities associated with the system, repeating the foregoing steps to compute adjusted risk values for the additional vulnerabilities (Fox, Col. 10, Lines 23 – 27) and calculating an adjusted security score for the host based on at least one of the adjusted risk values associated

Art Unit: 2134

with the host (Fox, Col. 10, Lines 3 - 36) but fails to teach computing an adjusted risk value as a function of the risk value and a fix difficulty value, the fix difficulty value indicating the difficulty of remedying the vulnerability associated with the risk. However, Nessus teaches computing an adjusted risk value as a function of the risk value and a fix difficulty value, the fix difficulty value indicating the difficulty of remedying the vulnerability associated with the risk (Nessus, Page 3 section 3).

[048] At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Nessus' method of determining risk and fixability with Fox's system for assessing security in a network, because it offers the advantage of displaying the vulnerability to a system (Nessus, Page 3 section 3).

[049] As per claim 12 Fox as modified teaches using adjusted score to decide when to fix a host (Nessus, Page 3 section 3).

[050] As per claim 13 Fox as modified teaches calculating a group adjusted security score for a group of hosts on individual adjusted security scores (Fox, Col. 9 Lines 66-67, Col. 10 Lines 1 -22).

[051] As per claim 14 Fox as modified teaches a severity value based on the potential access available to the network from exploiting the vulnerability (Fox, Col. 10 Lines 5 - 36).

[052] As per claim 15 Fox as modified teaches the step of computing a risk value multiplying the asset value, the probability value and the severity value (Fox, Col. 10, lines 5- 36).

Art Unit: 2134

[053] As per claim 16 Fox as modified teaches the step of calculating a security score placing a risk value on a banded scale (Fox, Col. 9 Lines 61 – 65, Col. Lines 23 – 36).

[054] As per claim 17 Fox as modified teaches a computer-implemented medium having computer-executable instructions for performing the steps (Fox, Col. 3 Lines 52 – 57).

[055] As per claim 21 Fox as modified teaches calculating an adjusted risk value as a function of the risk and a fix difficulty value (Nessus, Page 3 section 3).

[056] As per claim 22 Fox as modified teaches calculating an adjusted security score for the system based on at least one adjusted risk value (Fox, Col. 4 Lines 13 – 20).

[057] As per claim 32 Fox fails to disclose a step of computing an adjusted risk value as a function of the risk value and a fix difficulty value. However, Nessus teaches a step of computing an adjusted risk value as a function of the risk value and a fix difficulty value (Nessus, Page 3 section 3).

[058] At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Nessus' method of determining risk and fixability with Fox's system for assessing security in a network, because it offers the advantage of displaying the vulnerability to a system (Nessus, Page 3 section 3).

[059] As per claims 33 Fox as modified discloses a step of calculating all adjusted security score from at least one adjusted risk value (Fox, Col. 4 Lines 13 – 20).

[060] As per claim 38 Fox as modified teaches receiving a vulnerability for a host, the vulnerability being identified during a security scan (Fox, Col. 3, Lines 32 – 36), obtaining an asset value for the host, the asset value based on at least one of a host

Art Unit: 2134

operating system, a host service, and the host vulnerability (Fox, Col. 3 Lines 31-36), determining an exploit probability for the vulnerability (Fox, Col. 9, Lines 43- 45), obtaining a severity value for the vulnerability (Fox, Col. 9, Lines 17 – 20), computing a risk value for the vulnerability based on at least one of the asset value, the exploit probability, and the severity value (Fox, Col. 10 Lines 5 – 10, 15 – 21), computing an adjusted risk value as a function of the risk value and a fix difficulty value (Nessus, Page 3 section 3), if there are additional vulnerabilities associated with the system, repeating the foregoing steps to compute adjusted risk values for the additional vulnerabilities (Fox, Col. 10, Lines 23 – 27), and calculating an adjusted security score for the host based on at least one of the adjusted risk values associated with the host (Fox, Col. 10, Lines 3 - 36).

[060] As per claim 39 Fox as modified discloses a computer-readable medium having further computer-executable instructions for performing the step of using the adjusted security score to decide when to fix a host (Fox, Col. 3, Lines 52 – 57).

[061] As per claim 40 Fox as modified discloses a computer-readable medium having further computer-executable instructions for performing the step of computing a group adjusted security score for a group of hosts based on an individual adjusted security scores (Fox, Col. 3, Lines 52 – 57, Col. 9 Lines 66 – 67, Col. 10 Lines 1 – 22).

As per claim 41 Fox as modified discloses a computer-readable medium having further computer-executable instructions for performing the step of computing a risk value by multiplying the asset value, the probability value and the severity value (Fox, Col. 3, Lines 52 – 57, Fox, Col. 10, lines 5- 36).

Art Unit: 2134

[062] As per claim 42 Fox as modified discloses a computer-readable medium having further computer-executable instructions for performing the step of calculating a security score by placing a risk value on a banded scale (Fox, Col. 9, Lines 61 – 65, Col. 10, Lines 23 – 36).

[063] Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fox et al. U.S. Patent No. (6,883,101) in view of Townsend U.S. Patent No. (6,374,358).

[064] As per claim 4 Fox fails to disclose using a security score to assess the need for repair of the system. However, Townsend teaches using a security score to assess the need for repair of the system (Townsend, Col. 3 Lines 59 – 65).

[065] At the time the invention was made, it would have been obvious to one of ordinary skill in the art to assess the need for a repair with, Fox's system for assessing security in a network because it offers the advantage of improving the assessment of information security in large corporate systems (Townsend, Col. 2 Lines 9 – 12).

Conclusion

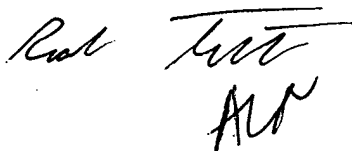
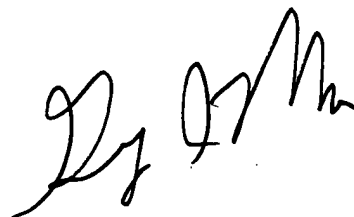
[066] Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on 8:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Roderick Tolentino

Handwritten signature of Roderick Tolentino in cursive script.Handwritten signature of Gregory Morse in cursive script.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2160